Computers and Electrical Engineering 70 (2018) 74–82

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Secure circuit with optical energy harvesting against unpowered physical attacks☆

Hyungseup Kim[a], Youngwoon Ko[a], Yeongjin Mun[a], Byeoncheol Lee[a], Dong Kyue Kim[b], Byong-Deok Choi[b], Ji-Hoon Kim[c], Hyoungho Ko[a,*]

[a] Department of Electronics Engineering, Chungnam National University, Daejeon 34134, Republic of Korea
[b] Department of Electronic Engineering, Hanyang University, Seoul 04763, Republic of Korea
[c] Department of Electronic and Electrical Engineering, Ewha Womans University, Seoul 03760, Republic of Korea

ARTICLE INFO

Keywords:
Optical energy harvesting
Optical secure circuit
On-chip photodiode
Hardware security
Physical attack protection

ABSTRACT

This study presents an optical secure circuit for physical attack protection. On-chip photodiodes are integrated for optical energy harvesting to operate the optical secure circuit in a standard CMOS process. The aim of the proposed optical secure circuit is to protect the secure contents of the IC against external unpowered attacks. When invasive unpowered physical attacks such as decapsulation are attempted, the photodiodes accumulate charge from ambient light and activate the secure circuit path that shuts down the secure data path. The proposed secure circuit is fabricated using a standard 0.18 μm 1P6M CMOS process with a small active area of 0.34 mm^2 with fully integrated on-chip photodiodes. When the chip is decapsulated and unpowered, the supply voltage of 600 mV with the ambient light is generated by the optical harvester, and the security data paths are shut down in 500 ns.

1. Introduction

Physical attacks such as decapsulation, focused ion beam (FIB) chip editing, and microprobing are threats to integrated circuits (ICs) with secure data. The physical attacks are classified as non-invasive and invasive attacks. Timing attacks, brute force attacks, power analysis, electro-magnetic analysis (EMA), and glitch attacks are classified as non-invasive attacks; Optical imaging, decapsulation, FIB with chip modification, and reverse engineering are classified as invasive attacks. Due to technological advancements, unpowered invasive attacks can become unstoppable even if there are secure protecting blocks on the IC to protect critical information. Unpowered physical attacks such as microprobing, which obtain signal information of the attacked chip, can easily probe parallel signals instantly and modify the signal states by forcing a specific value to the probing path constantly [1,2]. To protect the chip from microprobing, several protection techniques have been presented [3–15,18–20]. A camouflaging technique has been presented to obstruct attacks such as imaging-based reverse engineering [3–9]. This technique implements dummy gates into combinational logic gates to make it undetectable by imaging-based reverse engineering. Camouflaging is intended to confuse the attacker inspecting the layout of the decapsulated IC. The camouflaged gates make it difficult for the attacker to identify the schematic configuration of the attacked IC by implementing dummy contacts, filler cells, and a programmable standard cell [7–9]. A 64-kB logic resistive random access memory (RRAM) was implemented for secure key storage with security features of resisting invasive attacks such as decapsulation and microscopy observation [10]. Top metal shielding to protect the secured IC part by

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. J-S Sheu.

* Corresponding author.
E-mail address: hhko@cnu.ac.kr (H. Ko).

https://doi.org/10.1016/j.compeleceng.2018.06.005
Received 15 September 2017; Received in revised form 7 June 2018; Accepted 8 June 2018

shielding the inner circuit with top metal has been presented [11–15]. Top metal shielding is a technique to stop a microprobing attempt by shielding the protected IC with a top metal. This technique protects the inner circuit information such as IC layout information, and data buses, which are shielded by the top metal from the microprobing attempt. Further, an active shield architecture based on top metal shielding has been presented [14–15]. However, top metal shielding can be bypassed by FIB chip editing [16–17]. A single-oscillator-based detector or probing-attempt detector has also been presented [18–20]. These detectors can detect microprobing attempts by using the phase difference caused by the load capacitance change introduced by probing between the victim and reference lines. However, the probing attempt detection method can be bypassed through reverse engineering such as decapsulation and FIB chip editing by neutralizing the detection paths. Therefore, there is a need for a technology that protects the secure data and completely disables the effects of the above-stated unpowered physical attacks.

This study presents an optical secure circuit with optical energy harvesting for physical attack protection. On-chip photodiodes are integrated for optical energy harvesting to operate the optical secure circuit in a standard complementary metal-oxide-semiconductor (CMOS) process. The purpose of the proposed optical secure circuit is to protect the secure contents of the IC against external unpowered attacks such as decapsulation and microprobing. When the invasive unpowered physical attacks such as decapsulation are attempted, the photodiodes accumulate charge from ambient light and activate the secure circuit path that shuts down the secure data path, making them inaccessible to microprobing attempts. The conventional optical energy harvesting schemes are generally implemented with an on-chip photodiode and a DC-DC converter [21]. The use of a DC-DC converter for optical energy harvesting increases the circuit complexity and requires a large active area. In this study, a stacked photodiode that can generate the required high voltage without the DC-DC converter is proposed. The photocurrents generated by the stacked structure photodiodes result in operating voltage high enough for activating the secure protection path without the DC-DC converter. The proposed optical secure circuit has a simple scheme that consists of an on-chip stacked photodiode, a storage capacitor, pull-down resistors, and pull-down switches. To achieve small active area overheads, the pull-down resistors are implemented with a pseudo resistor scheme. The proposed secure circuit with optical energy harvesting is fabricated using a standard 0.18 μm 1-poly-6-metal (1P6M) CMOS process with a small active area of 0.34 mm^2 including fully integrated on-chip photodiodes. When the chip is decapsulated and unpowered, the supply voltage of 600 mV using the ambient light is generated by the optical harvester, and the security data paths are shut down in 500 ns.

The remainder of this paper is organized as follows: the circuit implementation of the proposed IC is presented in Section 2, the simulation results of the optical secure circuit for physical attack protection are described in Section 3, the measurement results of the optical secure circuit for physical attack protection are described in Section 4, and the conclusions are presented in Section 5.

2. Circuit implementation

2.1. Description of proposed secure circuit

The concept description of the proposed secure circuit with optical energy harvesting for physical attack protection is shown in Fig. 1. The packaged IC with secure data may be attacked by invasive unpowered physical attacks such as decapsulation and microprobing to acquire data from the decapsulated IC; the proposed secure circuit operates and protects the secure data from such invasive unpowered physical attacks. The proposed optical secure circuit operates when it is decapsulated and exposed to ambient light. The voltage generation block, which consists of the on-chip photodiode, enables the optical secure circuit when it is exposed to light. The photodiode exposed to ambient light generates photocurrents, which increase the voltage in the storage capacitor. The voltage generated by the light exposed photodiode turns on the pull-down switch and shuts down the multiple output signal paths to the pads. The proposed secure circuit can proceed to energy harvesting by using a simple structure with an on-chip photodiode, a

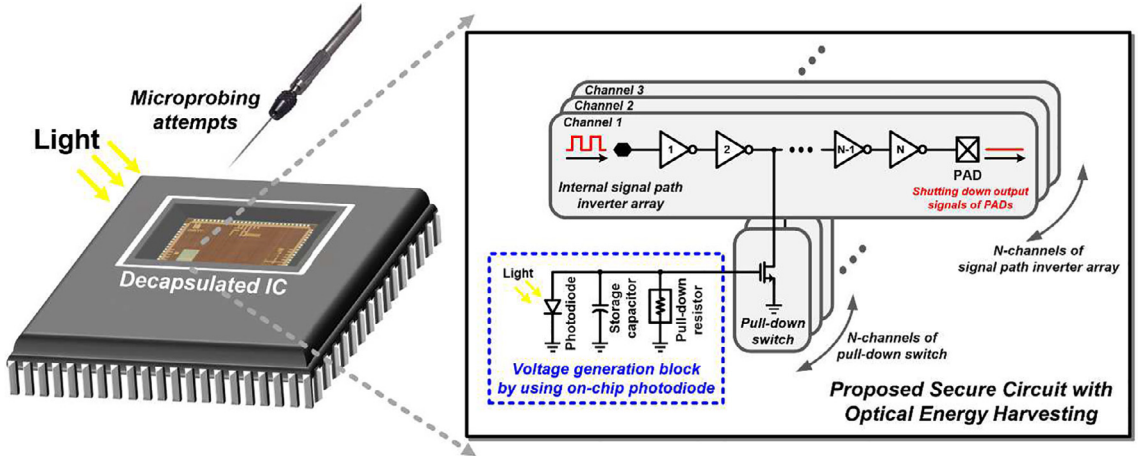

Fig. 1. Concept description of the proposed optical secure circuit.